ABSTRACT OF THE DISCLOSURE

A multi-word arithmetic device, capable of executing a variety of types of multi-word arithmetic required for elliptic curve cryptology, includes the following. A memory 40, formed from two dual-port memories 41 and 42, temporarily stores *n*-word integers on which calculation is performed, and a calculation result. An arithmetic unit 20 executes two or more types of calculation, including addition and multiplication, on each word, and outputs a one-word result. A memory input/output unit 30 supplies a maximum of three pieces of one-word data from the memory 40 to the arithmetic unit 20, while simultaneously storing a one-word calculation result from the arithmetic unit 20 in the memory 40. A control unit 10 controls the arithmetic unit 20 and the memory input/output unit 30 so as to have the arithmetic unit execute one of modular addition and Montgomery reduction on *n* words.